PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-067210

(43)Date of publication of application : 07.03.2003

(51)Int.Cl. G06F 11/00

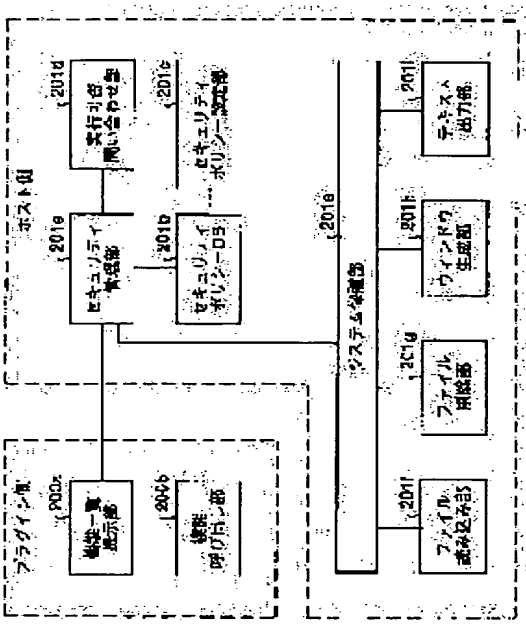
(21)Application number : 2001-251925

(22)Date of filing : 22.08.2001

(71)Applicant : JUST SYST CORP

(72)Inventor : TOYODA MITSUKI

(54) PROGRAM EXECUTION PREVENTION DEVICE, PROGRAM EXECUTION PREVENTION METHOD, PROGRAM FOR COMPUTER TO EXECUTE THE METHOD, AND COMPUTER READABLE RECORDING MEDIUM STORED WITH THE PROGRAM



(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the execution of a program dangerous to a user and a system, such as a virus infected program and a maliciously created program.

SOLUTION: Prior to installation or starting up of a plug-in, a function list showing unit 200a thereof shows to an application to be a host a list of functions (services) to be used by acquiring from the host. When a dangerous function (erasing a file, etc.), specified in advance in the list is included, a security management unit 201a of the host asks the user whether or not to still continue the installation/starting-up by an execution inquiry unit 201d. Also, during a plug-in execution, whether or not to continue the execution of the plug-in is inquired at any time when an actually requested function is not shown in the above list.

CLAIMS

[Claim(s)]

[Claim 1] A judgment means to judge whether the function specified by said assignment means is included in an assignment means by which a user's permission specifies a required function as the activation, and the functional listing shown from the program, The program execution arrester characterized by having an inquiry means to ask a user whether install said program when judged with said specified function being included in said functional listing by said judgment means.

[Claim 2] A judgment means to judge whether the function specified by said assignment means is included in an assignment means by which a user's permission specifies a required function as the activation, and the functional listing shown from the program, The program execution arrester characterized by having an inquiry means to ask a user whether start said program when judged with said specified function being included in said functional listing by said judgment means.

[Claim 3] The 1st judgment means which judges whether it is the function in which the function called from the program was specified as an assignment means by which a user's permission specifies a required function as the activation, by said assignment means, The 2nd judgment means which judges whether it was contained in the functional listing shown said function by which call appearance was carried out from said program when judged with said function by which call appearance was carried out being said specified function by said 1st judgment means, An inquiry means to ask a user whether continue said program execution when judged with not having been contained in the functional listing shown said function by which call appearance was carried out from said program by said 2nd judgment means, The program execution arrester characterized by preparation ******.

[Claim 4] The judgment process which judges whether the function specified at said assignment process is included in the assignment process to which a user's permission specifies a required function as the activation, and the functional listing shown from the program, The program execution prevention approach characterized by including the inquiry process which asks a user whether install said program when judged with said specified function being included in said functional listing at said judgment process.

[Claim 5] The judgment process which judges whether the function specified at said assignment process is included in the assignment process to which a user's permission specifies a required function as the activation, and the functional listing shown from the program, The program execution prevention approach characterized by including the inquiry process which asks a user whether start said program when judged with said specified function being included in said functional listing at said judgment process.

[Claim 6] The 1st judgment process which judges whether it is the function in which the function called from the program was specified as the assignment process to which a user's permission specifies a required function as the activation at said assignment process, The 2nd judgment process which judges whether it was contained in the functional listing shown said function by

which call appearance was carried out from said program when judged with said function by which call appearance was carried out being said specified function at said 1st judgment process, The inquiry process which asks a user whether continue said program execution when it judges that it was not contained in the functional listing shown from said program by said function by which call appearance was carried out at said 2nd judgment process, it is ****** -- the program execution prevention approach characterized by things.

[Claim 7] The program which makes a computer perform the approach of any one publication of said claim 4 - claim 6.

[Claim 8] The record medium which recorded said program according to claim 7 and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the record medium which recorded the program execution arrester which prevents beforehand a user or program execution dangerous for a system, the program execution prevention approach, the program which makes a computer perform that approach, and its program and in which computer reading is possible.

[0002]

[Description of the Prior Art] Although maintenance of the network (LAN) which connects the computer of the premises mutually from early was progressing in large-scale organisms, such as a company and a university, since the client/server system of PC base can introduce easily and cheaply, also in small and medium-sized enterprises, the individual house yard, etc., the network of two or more of the computers to hold is progressing quickly in recent years.

[0003] Moreover, the computer has become rather more common [being used accessing the Internet] rather than being used by the stand-alone by explosive expansion of the Internet for the past several years. Furthermore, connection also becomes less new and not only the number of the computer connected to the Internet but the connect time of each computer is always in the inclination which increases increasingly recently.

[0004] However, the data exchange with other computers in a network is one side of the convenience, and is also sponsoring the opportunity of best growth to the computer virus which trespassed upon the network concerned. The "I love you" virus (correctly worm) which spread in May, last year all over the world spreads, while winking through the e-mail system of the Internet, and the total amount of the material and immaterial damage which this generated measures, and is not found.

[0005]

[Problem(s) to be Solved by the Invention] And although the software for virus detection and extermination was also marketed in order to avoid generating of damage by such virus beforehand, the detection and extermination by this were surely "followed", and there were troubles, such as

that it cannot respond and becoming a "pinching game" with the virus of the new species which it is developed one after another and made skillful, in a strange virus on the principle.

[0006] That is, by such software, the existence of a code group (pattern) peculiar to a specific virus about all the possible locations of viral infections, such as a boot sector, a system memory, a partition table, and a file, is checked, and a virus is specified from the discovered code group.

[0007] When the user has neglected renewal of a chart as well as the virus which is not all over the chart which matched the virus and the code group of the proper, for example, the strange virus which is not discovered and analyzed once until now, even if it is a known virus since it is such a principle, it cannot detect and exterminate.

[0008] Moreover, Mutation Although the virus of the pleiomorphia mold which gets used even to which of the gestalt of 4 billion is increasing since the release of Engine (software with which a simple virus is easily changed into the implementer of a virus by the pleiomorphia mold), since the code group contained in this type of virus is changing from the original thing, the detection and extermination by the above-mentioned technique become difficult.

[0009] Furthermore, the above-mentioned software has the essential problem that a program with a certain malice without a virus and great difference is undistinguishable from the program which is not so, in that a damage is chiefly given to a user and a system for the purpose of detection and extermination of a virus. For example, unless all ActiveX controls which change a dialup place freely, and programs prepared in order to automate a setup and modification of a dialup place are infected with the virus, activation will be permitted similarly.

[0010] Based on the security policy for every environment of that, there are some which have restricted access to a local resource depending on this point environment. For example, the Java applets (i application etc.) performed on VM of Java cannot access the files on the computer which operates (for example, telephone directory etc.) at all.

[0011] From a viewpoint of safety, this is the very powerful and positive defense approach, but on the other hand it serves as big failure and limit in development of practical application, and has the problem that the convenience of a developer or a user is spoiled.

[0012] This invention aims at offering the record medium which recorded a program dangerous for a user or a system or the program execution arrester which can prevent activation of that problem part beforehand at least, the program execution prevention approach, the program which makes a computer perform that approach, and its program and in which computer reading is possible.

[0013]

[Means for Solving the Problem] In order to solve the technical problem mentioned above and to attain the purpose, the program execution arrester concerning invention according to claim 1 A judgment means to judge whether the function specified by said assignment means is included in an assignment means by which a user's permission specifies a required function as the activation, and the functional listing shown from the program, When judged with said specified function being included in said functional listing by said judgment means, it is characterized by having an inquiry means to ask a user whether install said program.

[0014] While being warned to a user of that fact in advance of install about the program which

performs processing specified beforehand according to this invention according to claim 1, the install concerned is stopped when a user directs.

[0015] Moreover, a program execution arrester according to claim 2 A judgment means to judge whether the function specified by said assignment means is included in an assignment means by which a user's permission specifies a required function as the activation, and the functional listing shown from the program, When judged with said specified function being included in said functional listing by said judgment means, it is characterized by having an inquiry means to ask a user whether start said program.

[0016] While being warned to a user of that fact in advance of starting about the program which performs processing specified beforehand according to this invention according to claim 2, the starting concerned is stopped when a user directs.

[0017] Moreover, a program execution arrester according to claim 3 The 1st judgment means which judges whether it is the function in which the function called from the program was specified as an assignment means by which a user's permission specifies a required function as the activation, by said assignment means, The 2nd judgment means which judges whether it was contained in the functional listing shown said function by which call appearance was carried out from said program when judged with said function by which call appearance was carried out being said specified function by said 1st judgment means, When judged with not having been contained in the functional listing shown said function by which call appearance was carried out from said program by said 2nd judgment means, it is characterized by having an inquiry means to ask a user whether continue said program execution.

[0018] When a different function from having been beforehand shown among program execution is called according to this invention according to claim 3, while being warned to a user of that fact, when a user directs, the program execution concerned is interrupted.

[0019] Moreover, the program execution prevention approach according to claim 4 The judgment process which judges whether the function specified at said assignment process is included in the assignment process to which a user's permission specifies a required function as the activation, and the functional listing shown from the program, When judged with said specified function being included in said functional listing at said judgment process, it is characterized by including the inquiry process which asks a user whether install said program.

[0020] While being warned to a user of that fact in advance of install about the program which performs processing specified beforehand according to this invention according to claim 4, the install concerned is stopped when a user directs.

[0021] Moreover, the program execution prevention approach according to claim 5 The judgment process which judges whether the function specified at said assignment process is included in the assignment process to which a user's permission specifies a required function as the activation, and the functional listing shown from the program, When judged with said specified function being included in said functional listing at said judgment process, it is characterized by including the inquiry process which asks a user whether start said program.

[0022] While being warned to a user of that fact in advance of starting about the program which

performs processing specified beforehand according to this invention according to claim 5, the starting concerned is stopped when a user directs.

[0023] Moreover, the program execution prevention approach according to claim 6 The 1st judgment process which judges whether it is the function in which the function called from the program was specified as the assignment process to which a user's permission specifies a required function as the activation at said assignment process, The 2nd judgment process which judges whether it was contained in the functional listing shown said function by which call appearance was carried out from said program when judged with said function by which call appearance was carried out being said specified function at said 1st judgment process, When it judges that it was not contained in the functional listing shown from said program by said function by which call appearance was carried out at said 2nd judgment process, it is characterized by including the inquiry process which asks a user whether continue said program execution.

[0024] When a different function from having been beforehand shown among program execution is called according to this invention according to claim 6, while being warned to a user of that fact, when a user directs, the program execution concerned is interrupted.

[0025] Moreover, a program according to claim 7 is characterized by being the program which makes a computer perform the approach of any one publication of said claim 4 - claim 6.

[0026] According to this invention according to claim 7, the approach of any one publication of said claim 4 - claim 6 is read by computer, and is performed.

[0027] Moreover, a record medium according to claim 8 is characterized by recording said program according to claim 7.

[0028] According to this invention according to claim 8, said approach according to claim 7 is read by computer, and is performed.

[0029]

[Embodiment of the Invention] The gestalt of suitable operation of the record medium which recorded the program execution arrester by this invention, the program execution prevention approach, the program that makes a computer perform that approach, and its program on below with reference to the accompanying drawing and in which computer reading is possible is explained to a detail.

[0030] Drawing 1 is the explanatory view showing the hardware configuration of the program execution arrester concerning the gestalt of operation of this invention. In this drawing, RAM for which 103 is used as a work area of CPU101 in ROM 102 remembered the intercalation output program to be for CPU by which 101 controls the whole equipment is shown, respectively.

[0031] Moreover, HD which memorizes the data with which HDD (hard disk drive) by which 104 controls the read/write of the data to HD (hard disk)105 according to control of CPU101 was written in 105 according to control of HDD104 is shown, respectively. Moreover, FD which can be detached and attached and which memorizes the data with which FDD (floppy disk drive) by which 106 controls the read/write of the data to FD (floppy (trademark) disk)107 according to control of CPU101 was written in 107 according to control of FDD106 is shown, respectively.

[0032] Moreover, the network interface on which it connects with a network through a

telecommunication cable 110, and 109 functions the display whose 108 displays various data, such as cursor, a menu, a window or an alphabetic character, and an image, as an interface of a network and CPU101 concerned is shown, respectively.

[0033] Moreover, the mouse with which 112 performs the keyboard with which 111 was equipped with two or more keys for inputs, such as an alphabetic character, a numeric value, and various directions, for selection of various directions, activation and selection of a processing object, migration of cursor, etc. is shown, respectively. Moreover, a bus or a cable for 100 to connect each part of the above for the CD-ROM drive with which 114 controls the lead of data [as opposed to CD-ROM113 for CD-ROM which is a record medium with removable 113] is shown, respectively.

[0034] Next, drawing 2 is the explanatory view showing functionally the configuration of the program execution arrester concerning the gestalt of operation of this invention. the program execution arrester by this invention is specifically explained to be (1) plug-in below -- as -- (2) -- the activation propriety of the plug-in concerned is judged, and when activation is good, application (application which serves as a host) which provides the plug-in concerned with various functions (service) is realized more. And 200x are a function part realized with plug-in by the application with which 201x become the host, respectively among drawing 2 .

[0035] 200a is the functional listing presentation section which shows the application which serves as the host the list of the functions which the plug-in concerned uses just before install of plug-in, or starting. Or it shows the list of the functions in which it is planned that this plug-in calls from the host concerned at the time of a handshake with a host but is good. Actually, the installer of the plug-in concerned will perform functional presentation before install, and the body of the plug-in concerned will perform functional presentation before starting after install.

[0036] Moreover, 200b is the functional call section in which call the various functions (for example, services, such as file reading, file deletion, window generation, and a text output) which a host offers according to a predetermined procedure, and processing by each function is made to perform.

[0037] Next, 201a is the security management section which judges the install propriety and starting propriety, or continuation propriety (these are also collectively called activation propriety below) before activation of the plug-in concerned, or during activation with reference to the functional listing shown from functional listing presentation section 200a of plug-in.

[0038] Moreover, 201b is the security policy DB (database) used as the foundation of the judgment by security management section 201a which stores a security policy. There are a thing for judging that activation propriety (install propriety or starting propriety) before activation of (1) plug-in and a thing for judging that activation propriety (continuation propriety) during activation of (2) plug-in at this security policy.

[0039] Specifically with the security policy before activation of (1) "when the specific function is included in the functional listing shown from the plug-in concerned before activation of plug-in It asks [whether the plug-in concerned is installed and] a user whether start or not." with the security policy under activation of (2) "When the function which is not into the functional listing which is the above-mentioned specific function during activation of plug-in, and was shown before activation from the plug-in concerned is called, it asks a user whether continue activation of the

plug-in concerned."
[0040] Next, 201c is the security policy setting section which stores the set-up information in security policy DB201b while receiving a detail setup of the above-mentioned security policy from a user.
[0041] Drawing 3 is an explanatory view which is displayed by security policy setting section 201c and in which showing an example of the screen for setting up "the specific function" of the security policy of the above (1) and (2). Those to which a possibility of giving a damage to a user and a system among the functions with which the plug-in is provided has the application which serves as a host in the box 300 of the left-hand side in drawing are enumerated.
[0042] For example, a system file and other data files may be deleted without a user's permission by activation of the plug-in concerned a "deleting file which another program created" (refer to drawing 3)-by calling host's function case. [plug-in of a certain mailer] This may cause the serious situations -- all of the abnormalities and destruction of a system, and mail have been erased.
[0043] Moreover, if another program in which a host does not have a concern will be started when plug-in "can call another program", it is not known what kind of destructive action the program carries out henceforth. Since system information and individual humanity news are stored in registry when "registry can be accessed", damage -- the individual humanity news (especially password) which can change the dial-up connection place which has a system destroyed is stolen -- may occur.
[0044] Moreover, also when "e-mail can be sent to the user who is not registered into an address book", the individual humanity news of users including a mail address may flow into a strange partner. On the contrary, also when "e-mail can be sent to all the users registered into the address book", there is a possibility that the damage of a virus may be continuously expanded from an acquaintance to an acquaintance so that the example of "I love you" which was much in fashion in the spring of last year may show.
[0045] in addition -- if transmission places are a large number to some extent -- not necessarily -- all the users in an address book -- not but -- ** -- that with the same risk (like "Melissa", there are some which send a self duplicate to the first address of 50 affairs) -- it is -- here -- "-- all -- " -- you may be "more than O people" instead.
[0046] Moreover, since it can also regard as the combination of two functions with transmission of the mail to the member which carried out listing of the member from (1) address book, and (2) listings to transmitting e-mail to all the users in an address book, the above-mentioned expression can also be put in another way as "Members can be enumerated from an address book and e-mail can be transmitted" etc.
[0047] however, a known partner -- be -- a strange partner -- be -- since it will be thought that there is no risk if the text and transmission place are shown to a user and it is transmitted in the condition as it is in advance of transmission of e-mail (namely, ** to which neither alteration of the text nor attachment of a new file is performed), you may make it except such an exceptional case from the above in detail more finely
[0048] It may be indispensable for many functions shown in drawing 3 not to be accompanied by the

always above risk, and to use the function concerned on the purpose of the plug-in. Moreover, if it refers to the purpose of plug-in, a user may be able to judge the existence of danger separately. For example, if it is plug-in only for only displaying the image file of a certain format, when it is not necessary to delete other files clearly and the plug-in concerned is calling the function of file deletion temporarily, possibility of being infected with a certain virus is high.

[0049] Then, among the functions to enumerate in the box 300 on the left-hand side of drawing 3 , it is dangerous and the check extracts especially only what the need and a user consider in the right-hand side box 303 in advance with the right arrow carbon button 301 and the left arrow carbon button 302. As the above-mentioned specific function, this drawing is the example which specified "e-mail can be sent to all the users registered into the address book." If the O.K. carbon button 304 is pushed in this condition, security policy setting section 201c stores the contents of a setting in security policy DB201b.

[0050] When 201d is the activation propriety inquiry section and security management section 201a judges with an user validation being required at return and the next based on the security policy in security policy DB201b to drawing 2 , the dialog for acquiring the check is displayed.

[0051] Drawing 4 is the explanatory view showing an example of the dialog for checking the activation propriety before plug-in activation displayed by 201d of activation propriety inquiry sections. The function (good [extracted / in the right-hand side box 303 / from the left-hand side box 300 but]) and match which the user specified on the screen of drawing 3 are shown in this dialog among the functional listing which plug-in presented. And although processing which is called e-mail transmission to all the users in an address book and which cannot necessarily be said as insurance is performed so that this plug-in may be illustrated, the user is asked about whether it is still used.

[0052] in addition -- although the dialog of drawing 4 may be displayed any time as long as it is before activation of plug-in -- realistic -- (1) -- just before install of the plug-in concerned, and/or (2) -- it will display just before starting of the plug-in concerned.

[0053] And when a user pushes the "yes" carbon button 400 by the check in front of install (i.e., when a user permits use of the plug-in concerned in spite of warning), 201d of activation propriety inquiry sections displays a dialog as further shown in drawing 5, and after making it set up whether the again same check is also performed just before starting of plug-in, they install the plug-in concerned.

[0054] In addition, when a user pushes the "no" carbon button 401 in the dialog shown in drawing 4 , install displays the message of "having stopped install of plug-in", without carrying out.

[0055] Moreover, when the "yes" carbon button 500 is pushed in the dialog shown in drawing 5 (i.e., when it is set up so that it may also check just before starting), whenever plug-in installed after this is called by that host, the same dialog as drawing 4 comes to be displayed.

[0056] And when the "yes" carbon button 400 is pushed in the dialog of this drawing displayed just before starting, the plug-in concerned is started, without displaying the dialog of drawing 5 . Moreover, if the "no" carbon button 401 is pushed here, starting of plug-in will not be performed but will display the message of "were not able to start plug-in" instead.

[0057] Moreover, drawing 6 is the explanatory view showing an example of the dialog for checking the activation propriety during plug-in activation similarly displayed by 201d of activation propriety inquiry sections. This dialog is displayed at any time, when the function which is not into the functional listing which is the function which the user specified on the screen of drawing 3 during activation of plug-in, and was shown before activation is called.

[0058] Only according to the check before the activation by the security policy of (1) mentioned above (just before install or starting), when infected with the virus which plug-in can show the functional listing of camouflage, a monitor will be able to be easily escaped by not notifying a dangerous function. Then, also while performing whether the function which differs from having been shown before activation by the above-mentioned (2) security policy is called, it monitors continuously.

[0059] In the example of drawing 6 , although e-mail transmission to all the users in an address book was not notified in advance, activation of the above-mentioned function will be suspended by the display of the above-mentioned dialog during activation of the plug-in concerned temporarily, and, so to speak, it will be stopped at the water's edge.

[0060] In addition, the user who received warning by the dialog of drawing 6 can perform processing shown in the dialog as it is by carrying out the depression of the "continuation" carbon button 600, if it judges that it is satisfactory. Moreover, when it judges that there is a certain risk, activation of this plug-in can once be interrupted for carrying out the depression of the "termination" carbon button 601, and the measures of reconfirming the source of plug-in can be taken.

[0061] But if it is planned to say that no doubtful plug-in which calls the function which has not been notified in advance is used, the plug-in concerned is directly uninstallable from the dialog of this drawing by carrying out the depression of the "uninstallation" carbon button 602.

[0062] If 201e is the system-protection section and the call of one of functions is received from the functional call section 200b during activation of plug-in to drawing 2 at return and the next, it will be asked to security management section 201a whether the function concerned is what activation is permitted without an user validation.

[0063] And when activation is permitted under the above-mentioned (2) security policy (i.e., when the function concerned is notified in advance), system-protection section 201e is directed to one which provides plug-in with the function concerned of function parts (after-mentioned), and makes the demanded processing perform.

[0064] Moreover, when activation of the function concerned is not permitted (i.e., when the function concerned is not what was notified in advance), a dialog as shown in drawing 6 is displayed by 201d of activation propriety inquiry sections which received the directions from security management section 201a. And when "continuation" carbon button 600 is pushed in this dialog as mentioned above, system-protection section 201e is directed to one which provides plug-in with the above-mentioned function of function parts (after-mentioned), and makes the demanded processing perform.

[0065] 201f-201i are function parts to which they provide drawing 2 with various kinds of functions (service) to plug-in next, and the file reading section which offers 201f of services of file reading to

return, the file cutout which offers 201g of services of file deletion, the window generation section which offers 201h of services of window generation, and 201i are the text output section offered in service of a text output. In addition, although much functions offered exist besides what was hung up above, illustration is omitted in this drawing (for example, registry access, e-mail transmission, etc.).

[0066] Next, drawing 7 - drawing 9 are flow charts in the program execution prevention system concerning the gestalt of operation of this invention which show the procedure of program execution prevention processing. The termination of install of a program (in this case, plug-in) and drawing 8 prevent the termination of starting of a program (this left), and, as for drawing 9 , drawing 7 prevents program execution respectively dangerous as a result by interruption of the program under activation (this left).

[0067] In addition, in advance of initiation of processing by the flow chart of this 7- drawing 9 , the security policy before activation and under activation shall be beforehand set as security policy DB201b by security policy setting section 201c.

[0068] The procedure of the program execution prevention by the termination of install first shown in drawing 7 is explained. Functional listing presentation section 200a of plug-in presents the list of the functions which the plug-in concerned calls and uses in advance of install of the plug-in concerned to the application which serves as the host (step S701).

[0069] While the application which serves as a host receives the above-mentioned list by that security management section 201a, with reference to the security policy in security policy DB201b, an user validation judges whether it is the need to install of this plug-in (step S702). if it specifically checks and includes whether the function specified beforehand is included during the shown list -- a check important point -- if not contained -- a check -- suppose that it is unnecessary.

[0070] And if the user validation is required (step S702: Yes), a dialog as shown in drawing 4 by 201d of activation propriety inquiry sections is displayed (step S703), and when the "yes" carbon button 400 is pushed in the dialog of this drawing, (step S704:Yes) and a dialog as further shown in drawing 5 will be displayed (step S705). Then, it carries out usually through install of the plug-in concerned (step S706), and processing by this flow chart is ended.

[0071] Moreover, instead of performing (step S704:No) and install, when the "no" carbon button 401 is pushed in the dialog of drawing 4 , the message of the purport which stopped install is displayed (step S707), and processing by this flow chart is ended.

[0072] The procedure of the program execution prevention by motive termination shown in drawing 8 below is explained. If plug-in is called from the application which serves as the host, the functional listing presentation section 200a will show the list of functions which is planning use (step S801). In a host, an user validation judges whether it is the need in advance of starting of this plug-in by that security management section 201a (step S802).

[0073] When the function beforehand specified in the functional listing which is the dialog (step S705 of drawing 7) of drawing 5 at the time of install, and is the case where it is set up so that it may also check again just before starting, and was specifically shown above is included, it judges with an user validation being required (step S802: Yes). And it directs in 201d of activation

propriety inquiry sections, and a dialog as shown in drawing 4 is displayed (step S803).
[0074] If the "yes" carbon button 400 is pushed in this dialog (step S804: Yes), it will start usually through plug-in (step S805), and if the "no" carbon button 401 is pushed (step S804: No), after displaying the message of the purport which stopped starting of plug-in (step S806), processing by this flow chart is ended.
[0075] The procedure of the program execution prevention by activation interruption shown in drawing 9 below is explained. System-protection section 201e directs that there is a call of a function from functional call section 200b of plug-in to the application which serves as the host to security management section 201a, and it is made to judge whether the function concerned is what may be performed without an user validation (step S902). (step S901)
[0076] Security management section 201a is the function in which the function concerned was beforehand specified by security policy setting section 201c, and when it differs from the function shown before activation (just before install and/or starting), it judges with an user validation being required (step S902: Yes), and it is directed in 201d of activation propriety inquiry sections, and a dialog as shown in drawing 6 is displayed (step S903).
[0077] And if processing called when "continuation" carbon button 600 was pushed in this dialog (step S904: Yes) is performed, i.e., activation of plug-in is continued as it is (step S905) and the "termination" carbon button 601 is pushed (step S904: No, step S906:Yes), while interrupting activation of plug-in at that time, that fact will be displayed by the message (step S907).
[0078] Moreover, if "uninstallation" carbon button 602 is pushed (step S906: No), after uninstalling the plug-in concerned (step S908), processing by this flow chart will be ended.
[0079] In addition, when the function specified beforehand is included in the shown functional listing, or when [although it waited for directions of a user with the gestalt of operation mentioned above and an install termination, a starting termination, or activation interruption was carried out or] the function in which there is nothing into the functional listing shown beforehand is called, directions of a user are not waited but it may be made to carry out a termination and interruption compulsorily.
[0080] Moreover, although a setup of whether it checks to a user by the functional unit which a program uses, or not to carry out was performed with the gestalt of operation mentioned above (drawing 3), you may enable it to set up whether it checks for every program, or it does not carry out. For example, the management person in charge specifies plug-in beforehand, and when the other plug-in becomes installed, you may make it display warning like drawing 4 so that dangerous plug-in (plug-in which it is not in the law of a source) may not be easily introduced by other users when one PC is being used by two or more persons.
[0081] In addition, the program which realizes each above-mentioned function part can be stored in various record media, such as FD107 besides HD105, CD-ROM113, or MO, and can be distributed with the record medium concerned. Moreover, distributing through a network is also possible.
[0082] In addition, security management section 201a shown in drawing 2 is equivalent to the "judgment means", "the 1st judgment means", and "the 2nd judgment means" which are said to a claim, and the processing to perform is equivalent to the "judgment process", "the 1st judgment

process", and "the 2nd judgment process" which are said to a claim so that clearly also from the above-mentioned explanation.

[0083] Moreover, the processing to perform is equivalent to the "assignment process" said at a claim at the "assignment means" which security policy setting section 201c says to a claim. Furthermore, the processing to perform is equivalent to the "inquiry process" said at a claim at the "inquiry means" which 201d of activation propriety inquiry sections says to a claim.

[0084] Since install and starting of the plug-in concerned are refused according to decision of a user when the function in which there is a possibility of giving a damage to a user and a system is included in plug-in according to the gestalt of operation of this invention, as explained above, the damage which may be produced as a result of performing the plug-in concerned is beforehand avoidable.

[0085] Moreover, since the credibility is continuously monitored also during activation, without trusting easily the functional listing shown before activation, plug-in which it is going to call secretly while performing the dangerous function which has not been notified in advance can be stopped just before the function concerned is called. The effectiveness brought about by this is the same as that of the above.

[0086] And since the activation can be prevented if it does not ask whether this invention is the program created with whether it is the program infected with the virus on the principle, and a certain malice but dangerous actuation is carried out for a user or a system, the usual program which was difficult for indication, and a program with the malice which distinction does not attach are also easily detectable with the conventional technique.

[0087] Moreover, even if it is the virus of the pleiomorphia mold which is increasing in recent years, as long as the processing made into the purpose is the same, it has the features that it is detectable irrespective of the difference in an external code. And the activity which does not need to prepare the virus definition file (it is called a pattern file, a DAT file, etc.) which covered the code group of all viruses, and updates the file concerned frequently for the detection is also unnecessary.

[0088] Moreover, without requiring long duration like the conventional virus scan, since this invention prevents program execution by very simple judgment [say / whether a thing dangerous in the function which is a call schedule as mentioned above is contained, or the actually called function was notified in advance], it is enforced strictly reasonable every day and there is also a realistic merit that effectiveness can be planned.

[0089] Moreover, since the function which can be used like Java of the conventional technique is not restricted uniformly, the degree of freedom of a program is able to aim at coexistence of increase, safety, and convenience.

[0090] In addition, especially with the gestalt of operation mentioned above, activation propriety was judged about plug-in in the application which serves as the host in the program, and it is also possible to apply this invention, for example to the relation between a macro and the application concerned which carries out macro operation.

[0091] Moreover, this invention is applied between general applications and OS's, namely, the function of interruption of the program under the termination of install of a program, a motive

termination, or activation can also be given to the OS itself. By this, it will be equivalent to introducing antivirus software etc. separately, or the safety effectiveness beyond it will be acquired.
[0092] Drawing 10 is the explanatory view showing typically how activation of application is prevented, when OS is made to possess the program execution prevention function by this invention. This drawing shows the example interrupted when the application to which install and starting were once permitted calls during activation the file Delete function which is not during the above-mentioned list by presentation of the functional listing of camouflage.
[0093]
[Effect of the Invention] As explained above, invention according to claim 1 A judgment means to judge whether the function specified by said assignment means is included in an assignment means by which a user's permission specifies a required function as the activation, and the functional listing shown from the program, Since it had an inquiry means to ask a user whether install said program when judged with said specified function being included in said functional listing by said judgment means About the program which performs processing specified beforehand While being warned to a user of the fact in advance of install, the install concerned is stopped when a user directs. By this The effectiveness that the program execution arrester which can prevent program execution dangerous for a user or a system beforehand is obtained is done so.
[0094] Moreover, an assignment means by which invention according to claim 2 specifies a function to grant [of a user] a permission as the activation, A judgment means to judge whether the function specified by said assignment means in the functional listing shown from the program is included, Since it had an inquiry means to ask a user whether start said program when judged with said specified function being included in said functional listing by said judgment means About the program which performs processing specified beforehand While being warned to a user of the fact in advance of starting, when a user directs, the starting concerned is stopped and the effectiveness that the program execution arrester which can prevent dangerous program execution beforehand for a user or a system by this is obtained is done so.
[0095] Moreover, an assignment means by which invention according to claim 3 specifies a function to grant [of a user] a permission as the activation, The 1st judgment means which judges whether it is the function in which the function called from the program was specified by said assignment means, The 2nd judgment means which judges whether it was contained in the functional listing shown said function by which call appearance was carried out from said program when judged with said function by which call appearance was carried out being said specified function by said 1st judgment means, An inquiry means to ask a user whether continue said program execution when judged with not having been contained in the functional listing shown said function by which call appearance was carried out from said program by said 2nd judgment means, When a function which is different from having been beforehand shown among program execution by that of ******** is called While being warned to a user of the fact, when a user directs, the program execution concerned is interrupted. By this The effectiveness that the program execution arrester which can prevent beforehand activation of the problem part of a program dangerous for a user or a system is obtained is done so.

[0096] Moreover, the assignment process to which invention according to claim 4 specifies a function to grant [of a user] a permission as the activation, The judgment process which judges whether the function specified at said assignment process in the functional listing shown from the program is included, Since the inquiry process which asks a user whether install said program was included when judged with said specified function being included in said functional listing at said judgment process About the program which performs processing specified beforehand While being warned to a user of the fact in advance of install, the install concerned is stopped when a user directs. By this The effectiveness that the program execution prevention approach which can prevent program execution dangerous for a user or a system beforehand is acquired is done so.

[0097] Moreover, the assignment process to which invention according to claim 5 specifies a function to grant [of a user] a permission as the activation, The judgment process which judges whether the function specified at said assignment process in the functional listing shown from the program is included, Since the inquiry process which asks a user whether start said program was included when judged with said specified function being included in said functional listing at said judgment process About the program which performs processing specified beforehand While being warned to a user of the fact in advance of starting, when a user directs, the starting concerned is stopped and the effectiveness that the program execution prevention approach which can prevent dangerous program execution beforehand for a user or a system by this is acquired is done so.

[0098] Moreover, the assignment process to which invention according to claim 6 specifies a function to grant [of a user] a permission as the activation, The 1st judgment process which judges whether it is the function in which the function called from the program was specified at said assignment process, The 2nd judgment process which judges whether it was contained in the functional listing shown said function by which call appearance was carried out from said program when judged with said function by which call appearance was carried out being said specified function at said 1st judgment process, The inquiry process which asks a user whether continue said program execution when it judges that it was not contained in the functional listing shown from said program by said function by which call appearance was carried out at said 2nd judgment process, When a function which is different from having been beforehand shown among program execution by ****** is called While being warned to a user of the fact, when a user directs, the program execution concerned is interrupted. By this The effectiveness that the program execution prevention approach which can prevent beforehand activation of the problem part of a program dangerous for a user or a system is acquired is done so.

[0099] Moreover, since invention according to claim 7 makes a computer perform the approach of any one publication of said claim 4 - claim 6 The approach of any one publication of said claim 4 - claim 6 is read by computer, and is performed. By this The effectiveness that a program dangerous for a user or a system or the program which can prevent activation of the problem part beforehand at least is acquired is done so.

[0100] Moreover, since invention according to claim 8 recorded said program according to claim 7, said program according to claim 7 is read by computer, and is executed, and it does so the effectiveness that a dangerous program or the record medium which can prevent activation of the

problem part beforehand at least is obtained by this for a user or a system.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the explanatory view showing the hardware configuration of the program execution arrester concerning the gestalt of operation of this invention.

[Drawing 2] It is the explanatory view showing functionally the configuration of the program execution arrester concerning the gestalt of operation of this invention.

[Drawing 3] It is the explanatory view showing an example of the screen for setting up the detail of a security policy displayed by security policy setting section 201c.

[Drawing 4] It is the explanatory view showing an example of the dialog for checking the activation propriety before plug-in activation displayed by 201d of activation propriety inquiry sections.

[Drawing 5] It is the explanatory view showing an example of the dialog for setting up whether activation propriety is checked also just before starting of plug-in displayed by 201d of activation propriety inquiry sections.

[Drawing 6] It is the explanatory view showing an example of the dialog for checking the activation propriety during plug-in activation displayed by 201d of activation propriety inquiry sections.

[Drawing 7] It is the flow chart which shows the procedure of the program execution prevention processing by the termination of install in the program execution prevention system concerning the gestalt of operation of this invention.

[Drawing 8] It is the flow chart which shows the procedure of the program execution prevention processing by starting termination in the program execution prevention system concerning the gestalt of operation of this invention.

[Drawing 9] It is the flow chart which shows the procedure of the program execution prevention processing by activation interruption in the program execution prevention system concerning the gestalt of operation of this invention.

[Drawing 10] When this invention is applied to OS, it is the explanatory view showing typically how activation of application is prevented.

[Description of Notations]

100 Bus or Cable
101 CPU
102 ROM
103 RAM
104 HDD
105 HD
106 FDD
107 FD
108 Display
109 Network I/F

110 Telecommunication Cable

111 Keyboard

112 Mouse

113 CD-ROM

114 CD-ROM Drive

200a Functional listing presentation section

200b Functional call section

201a Security management section

201b Security policy DB

201c Security policy setting section

201d Activation propriety inquiry section

201e System protection section

201f File reading section

201g File cutout

201h Window generation section

201i Text output section

---

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－67210
（P2003－67210A）
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　11/00		Ｇ０６Ｆ　9/06	６６０Ｎ　５Ｂ０７６

審査請求　未請求　請求項の数８　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－251925(P2001－251925)

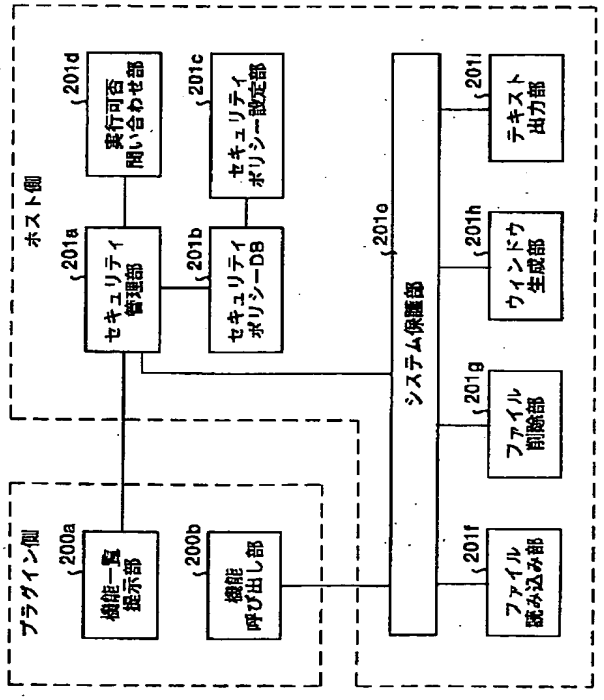
(22)出願日　平成13年８月22日(2001.8.22)

(71)出願人　390024350
株式会社ジャストシステム
徳島県徳島市沖浜東３－46
(72)発明者　豊田　光樹
徳島市沖浜東３丁目46番地　株式会社ジャストシステム内
(74)代理人　100104190
弁理士　酒井　昭徳

Ｆターム(参考)　5B076 FD08

(54)【発明の名称】　プログラム実行防止装置、プログラム実行防止方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　ウィルスに感染したプログラムや何らかの悪意をもって作成されたプログラムなど、ユーザやシステムにとって危険なプログラムの実行を未然に防止すること。
【解決手段】　プラグインのインストールあるいは起動に先立って、その機能一覧提示部２００ａはホストとなるアプリケーションに対し、当該ホストから呼び出して使用する機能（サービス）の一覧を提示する。ホストのセキュリティ管理部２０１ａは、上記一覧中にあらかじめ指定された危険な機能（ファイル削除など）が含まれる場合に、実行可否問い合わせ部２０１ｄによりそれでもインストール／起動をおこなうかどうかをユーザに問い合わせる。またプラグインの実行中には、実際に呼び出された機能が上記で提示されたものでなかった場合に、当該プラグインの実行を継続するかどうかを随時問い合わせる。



1

【特許請求の範囲】

【請求項１】　その実行にユーザの許可が必要な機能を指定する指定手段と、

プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、

前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ手段と、

を備えたことを特徴とするプログラム実行防止装置。

【請求項２】　その実行にユーザの許可が必要な機能を指定する指定手段と、

プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、

前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ手段と、

を備えたことを特徴とするプログラム実行防止装置。

【請求項３】　その実行にユーザの許可が必要な機能を指定する指定手段と、

プログラムから呼び出された機能が前記指定手段により指定された機能であるか否かを判定する第１の判定手段と、

前記第１の判定手段により前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第２の判定手段と、

前記第２の判定手段により前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ手段と、

を備えたことを特徴とするプログラム実行防止装置。

【請求項４】　その実行にユーザの許可が必要な機能を指定する指定工程と、

プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、

前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ工程と、

を含んだことを特徴とするプログラム実行防止方法。

【請求項５】　その実行にユーザの許可が必要な機能を指定する指定工程と、

プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、

2

前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ工程と、

を含んだことを特徴とするプログラム実行防止方法。

【請求項６】　その実行にユーザの許可が必要な機能を指定する指定工程と、

プログラムから呼び出された機能が前記指定工程で指定された機能であるか否かを判定する第１の判定工程と、

前記第１の判定工程で前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第２の判定工程と、

前記第２の判定工程で前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ工程と、

を含んだことを特徴とするプログラム実行防止方法。

【請求項７】　前記請求項４～請求項６のいずれか一つに記載の方法をコンピュータに実行させるプログラム。

【請求項８】　前記請求項７に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ユーザあるいはシステムにとって危険なプログラムの実行を未然に防止するプログラム実行防止装置、プログラム実行防止方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】企業や大学などの大規模な組織体では、早くからその構内のコンピュータを相互に接続するネットワーク（ＬＡＮ）の整備が進んでいたが、近年はＰＣベースのクライアント／サーバシステムが容易に、かつ安価に導入できることもあり、中小企業や個人家庭などにおいてもその保有する複数のコンピュータのネットワーク化が急速に進んでいる。

【０００３】また、ここ数年のインターネットの爆発的な拡大により、コンピュータはスタンドアロンで使用されるより、インターネットに接続されて使用されることのほうがむしろ一般的となってきた。さらに、最近は常時接続もめずらしくなくなり、インターネットに接続されたコンピュータの個数だけでなく、個々のコンピュータの接続時間もますます増大する傾向にある。

【０００４】ただ、ネットワーク内の他のコンピュータとのデータ交換は、その利便性の一方で、当該ネットワークに侵入したコンピュータ・ウィルスに対して絶好の増殖の機会を提供していることにもなる。昨年５月に世界中で蔓延した「Ｉ　ｌｏｖｅ　ｙｏｕ」ウィルス（正確にはワーム）は、インターネットのメールシステムを

通じてまたたく間に拡がり、それにより発生した有形・無形の被害の総額ははかりしれない。

【０００５】

【発明が解決しようとする課題】そして、このようなウィルスによる損害の発生を未然に回避するため、ウィルス検出・駆除のためのソフトウェアも市販されてはいるが、これによる検出・駆除はその原理上どうしても「後追い」となり、未知のウィルスには対応できないこと、次々と開発され巧妙化する新種のウィルスとの「いたちごっこ」になってしまうこと、などの問題点があった。

【０００６】すなわちこれらのソフトウェアでは、ブートセクタ、システムメモリ、パーティションテーブル、ファイルなど、ウィルス感染の可能性のあるあらゆる場所について、特定のウィルスに固有なコード群（パターン）の有無をチェックし、発見したコード群からウィルスを特定する。

【０００７】このような原理であるため、ウィルスとその固有のコード群とを対応づけた一覧表中にないウィルス、たとえばこれまで一度も発見・分析されたことのない未知のウィルスはもちろん、既知のウィルスであってもユーザが一覧表の更新を怠っている場合には、検出・駆除することができない。

【０００８】また、Ｍｕｔａｔｉｏｎ　Ｅｎｇｉｎｅ（ウィルスの作成者が単純なウィルスを容易に多形態型に変えられるソフトウェア）のリリース以来、４０億もの形態のどれにでもなれる多形態型のウィルスが増加しているが、このタイプのウィルスに含まれるコード群は本来のものから変容されているため、上記手法による検出・駆除が困難になる。

【０００９】さらに上記ソフトウェアはもっぱらウィルスの検出・駆除を目的とするものであって、ユーザやシステムにダメージを与えるという点ではウィルスと大差のない、何らかの悪意のあるプログラムを、そうでないプログラムと区別することはできないという本質的な問題を持っている。たとえば、ダイアルアップ先を勝手に変更してしまうＡｃｔｉｖｅＸコントロールと、ダイアルアップ先の設定・変更を自動化するために用意されたプログラムとは、いずれもウィルスに感染していない限りは同様に実行が許可されてしまう。

【００１０】この点環境によっては、その環境ごとのセキュリティポリシーにもとづいて、ローカルリソースへのアクセスを制限しているものがある。たとえばＪａｖａのＶＭ上で実行されるＪａｖａアプレット（ｉアプリなど）は、その動作するコンピュータ上のファイル（たとえば電話帳など）に一切アクセスすることができない。

【００１１】これは安全性という観点からは、非常に強力で確実な防御方法であるが、その反面で実用的アプリケーションの開発における大きな障害・制限となり、開発者やユーザの利便性が損なわれるという問題がある。

【００１２】この発明は、ユーザやシステムにとって危険なプログラム、あるいは少なくともその問題部分の実行を未然に防止することが可能なプログラム実行防止装置、プログラム実行防止方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００１３】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項１に記載の発明にかかるプログラム実行防止装置は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ手段と、を備えたことを特徴とする。

【００１４】この請求項１に記載の発明によれば、あらかじめ指定された処理をおこなうプログラムについては、インストールに先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該インストールが中止される。

【００１５】また、請求項２に記載のプログラム実行防止装置は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ手段と、を備えたことを特徴とする。

【００１６】この請求項２に記載の発明によれば、あらかじめ指定された処理をおこなうプログラムについては、起動に先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該起動が中止される。

【００１７】また、請求項３に記載のプログラム実行防止装置は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから呼び出された機能が前記指定手段により指定された機能であるか否かを判定する第１の判定手段と、前記第１の判定手段により前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第２の判定手段と、前記第２の判定手段により前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ手段と、を備えたことを特徴とする。

【００１８】この請求項３に記載の発明によれば、プロ

グラムの実行中あらかじめ提示されたのとは異なる機能が呼び出されたときは、ユーザにその事実が警告されるとともに、ユーザが指示した場合には当該プログラムの実行が中断される。

【００１９】また、請求項４に記載のプログラム実行防止方法は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ工程と、を含んだことを特徴とする。

【００２０】この請求項４に記載の発明によれば、あらかじめ指定された処理をおこなうプログラムについては、インストールに先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該インストールが中止される。

【００２１】また、請求項５に記載のプログラム実行防止方法は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ工程と、を含んだことを特徴とする。

【００２２】この請求項５に記載の発明によれば、あらかじめ指定された処理をおこなうプログラムについては、起動に先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該起動が中止される。

【００２３】また、請求項６に記載のプログラム実行防止方法は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから呼び出された機能が前記指定工程で指定された機能であるか否かを判定する第１の判定工程と、前記第１の判定工程で前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第２の判定工程と、前記第２の判定工程で前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ工程と、を含んだことを特徴とする。

【００２４】この請求項６に記載の発明によれば、プログラムの実行中あらかじめ提示されたのとは異なる機能が呼び出されたときは、ユーザにその事実が警告されるとともに、ユーザが指示した場合には当該プログラムの実行が中断される。

【００２５】また、請求項７に記載のプログラムは、前記請求項４～請求項６のいずれか一つに記載の方法をコンピュータに実行させるプログラムであることを特徴とする。

【００２６】この請求項７に記載の発明によれば、前記請求項４～請求項６のいずれか一つに記載の方法がコンピュータにより読み取られて実行される。

【００２７】また、請求項８に記載の記録媒体は、前記請求項７に記載のプログラムを記録したことを特徴とする。

【００２８】この請求項８に記載の発明によれば、前記請求項７に記載の方法がコンピュータにより読み取られて実行される。

【００２９】

【発明の実施の形態】以下に添付図面を参照して、この発明によるプログラム実行防止装置、プログラム実行防止方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００３０】図１は、本発明の実施の形態にかかるプログラム実行防止装置のハードウェア構成を示す説明図である。同図において、１０１は装置全体を制御するＣＰＵを、１０２は基本入出力プログラムを記憶したＲＯＭを、１０３はＣＰＵ１０１のワークエリアとして使用されるＲＡＭを、それぞれ示している。

【００３１】また、１０４はＣＰＵ１０１の制御にしたがってＨＤ（ハードディスク）１０５に対するデータのリード／ライトを制御するＨＤＤ（ハードディスクドライブ）を、１０５はＨＤＤ１０４の制御にしたがって書き込まれたデータを記憶するＨＤを、それぞれ示している。また、１０６はＣＰＵ１０１の制御にしたがってＦＤ（フロッピー（登録商標）ディスク）１０７に対するデータのリード／ライトを制御するＦＤＤ（フロッピーディスクドライブ）を、１０７はＦＤＤ１０６の制御にしたがって書き込まれたデータを記憶する着脱自在のＦＤを、それぞれ示している。

【００３２】また、１０８はカーソル、メニュー、ウィンドウ、あるいは文字や画像などの各種データを表示するディスプレイを、１０９は通信ケーブル１１０を介してネットワークに接続され、当該ネットワークとＣＰＵ１０１とのインターフェースとして機能するネットワークインターフェースを、それぞれ示している。

【００３３】また、１１１は文字、数値、各種指示などの入力のための複数のキーを備えたキーボードを、１１２は各種指示の選択や実行、処理対象の選択、カーソルの移動などをおこなうマウスを、それぞれ示している。また、１１３は着脱可能な記録媒体であるＣＤ－ＲＯＭを、１１４はＣＤ－ＲＯＭ１１３に対するデータのリードを制御するＣＤ－ＲＯＭドライブを、１００は上記各部を接続するためのバスまたはケーブルを、それぞれ示している。

【００３４】つぎに、図２は本発明の実施の形態にかかるプログラム実行防止装置の構成を機能的に示す説明図である。本発明によるプログラム実行防止装置は、具体的には（１）プラグインと、以下に説明するように（２）当該プラグインの実行可否を判定し、実行可である場合に当該プラグインに各種機能（サービス）を提供するアプリケーション（ホストとなるアプリケーション）、により実現される。そして、図２中２００ｘはプラグインにより、２０１ｘはそのホストとなるアプリケーションにより、それぞれ実現される機能部である。

【００３５】２００ａは、プラグインのインストール直前あるいは起動直前に、当該プラグインが使用する機能の一覧をそのホストとなるアプリケーションに提示する機能一覧提示部である。あるいは、ホストとのハンドシェーク時に、このプラグインが当該ホストから呼び出すことが予定されている機能の一覧を提示する、といってもよい。現実的には、インストールに先立っての機能提示は当該プラグインのインストーラがおこない、インストール後、起動に先立っての機能提示は当該プラグインの本体がおこなうことになる。

【００３６】また、２００ｂは所定の手続きにしたがって、ホストが提供する種々の機能（たとえばファイル読み込み、ファイル削除、ウィンドウ生成、テキスト出力などといったサービス）を呼び出し、各機能による処理をおこなわせる機能呼び出し部である。

【００３７】つぎに、２０１ａはプラグインの機能一覧提示部２００ａから提示された機能一覧を参照して、当該プラグインの実行前または実行中に、そのインストール可否や起動可否、あるいは継続可否（以下ではこれらをまとめて実行可否ともいう）を判定するセキュリティ管理部である。

【００３８】また、２０１ｂはセキュリティ管理部２０１ａによる判定の基礎となる、セキュリティポリシーを格納するセキュリティポリシーＤＢ（データベース）である。このセキュリティポリシーには、（１）プラグインの実行前にその実行可否（インストール可否あるいは起動可否）を判定するためのものと、（２）プラグインの実行中にその実行可否（継続可否）を判定するためのものとがある。

【００３９】具体的には、（１）の実行前のセキュリティポリシーとは、「プラグインの実行前、当該プラグインから提示された機能一覧中に特定の機能が含まれている場合に、当該プラグインをインストールするか否か、あるいは起動するか否かをユーザに問い合わせる」というものであり、（２）の実行中のセキュリティポリシーとは、「プラグインの実行中、上記特定の機能であって、かつ当該プラグインから実行前に提示された機能一覧中にない機能が呼び出された場合に、当該プラグインの実行を継続するか否かをユーザに問い合わせる」というものである。

【００４０】つぎに、２０１ｃは上記セキュリティポリシーの詳細設定をユーザから受け付けるとともに、設定された情報をセキュリティポリシーＤＢ２０１ｂに格納するセキュリティポリシー設定部である。

【００４１】図３は、セキュリティポリシー設定部２０１ｃにより表示される、上記（１）（２）のセキュリティポリシーの「特定の機能」を設定するための画面の一例を示す説明図である。図中左側のボックス３００には、ホストとなるアプリケーションがそのプラグインに提供する機能のうち、ユーザやシステムにダメージを与えるおそれのあるものが列挙されている。

【００４２】たとえばあるメーラーのプラグインが、ホストの機能を呼び出すことで「別のプログラムが作成したファイルを削除できる」（図３参照）場合、当該プラグインの実行によって、システムファイルやその他のデータファイルがユーザの許可なく削除されてしまう可能性がある。これはシステムの異常・破壊や、メールがすべて消されてしまったなどの深刻な事態を引き起こしかねない。

【００４３】また、プラグインが「別のプログラムを呼び出すことができる」場合、ホストが関知しない別のプログラムが起動されてしまえば、以後はそのプログラムがどんな破壊的な行動をするか分からない。「レジストリにアクセスできる」場合、レジストリにはシステム情報や個人情報が格納されているので、システムを破壊される、ダイアルアップの接続先を変えられる、個人情報（特にパスワード）を盗まれるなどの被害が発生しうる。

【００４４】また、「アドレス帳に登録されていないユーザにメールを送ることができる」場合も、メールアドレスをはじめとするユーザの個人情報が未知の相手に流出してしまう可能性がある。逆に、「アドレス帳に登録されているすべてのユーザにメールを送ることができる」場合も、昨年春に大流行した「Ｉ　ｌｏｖｅ　ｙｏｕ」の例から分かるように、知人から知人へと連鎖的にウィルスの被害が拡大するおそれがある。

【００４５】なお、送信先はある程度多数であれば、必ずしもアドレス帳内の全ユーザでなくとも同様の危険がある（「Ｍｅｌｉｓｓａ」のように、最初の５０件のアドレスへ自己の複製を送付するものもある）ので、ここは「すべて」の代わりに「○人以上」などであってもよい。

【００４６】また、アドレス帳内の全ユーザにメールを送信するとは、（１）アドレス帳からのメンバの列挙と、（２）列挙したメンバへのメールの送信との二つの機能の組み合わせと見ることもできるので、上記の表現は「アドレス帳からメンバを列挙してメールを送信することができる」などと言い換えることもできる。

【００４７】ただし既知の相手であれ未知の相手であれ、メールの送信に先立ってその本文や送信先がユーザ

に示され、かつそのままの状態で（すなわち、本文の改ざんや新たなファイルの添付などがおこなわれずに）送信されるならば危険はないと考えられるので、よりきめ細かに、上記からこうした例外的なケースを逐一除外するようにしてもよい。

【００４８】図３に示す諸機能は常に上記のような危険をともなうものではなく、そのプラグインの目的上、当該機能を使用することが必要不可欠な場合もある。また、プラグインの目的と照らし合わせれば、ユーザが個々に危険性の有無を判断できる場合もある。たとえば、単にある形式の画像ファイルを表示させるためだけのプラグインであれば、明らかに他のファイルを削除する必要はなく、仮に当該プラグインがファイル削除の機能を呼び出している場合、何らかのウィルスに感染している可能性が高い。

【００４９】そこで、図３の左側のボックス３００に列挙する機能のうち、特に危険であって事前に確認が必要とユーザが考えるものだけを、右矢印ボタン３０１と左矢印ボタン３０２により右側のボックス３０３に抽出しておく。同図は上記特定の機能として、「アドレス帳に登録されているすべてのユーザにメールを送ることができる」を指定した例である。この状態でＯＫボタン３０４が押下されると、セキュリティポリシー設定部２０１ｃは設定内容をセキュリティポリシーＤＢ２０１ｂに格納する。

【００５０】図２に戻り、つぎに２０１ｄは実行可否問い合わせ部であり、セキュリティ管理部２０１ａがセキュリティポリシーＤＢ２０１ｂ内のセキュリティポリシーにもとづき、ユーザの確認が必要と判定した場合に、その確認を得るためのダイアログを表示する。

【００５１】図４は、実行可否問い合わせ部２０１ｄにより表示される、プラグイン実行前にその実行可否を確認するためのダイアログの一例を示す説明図である。このダイアログには、プラグインが提示した機能一覧中、ユーザが図３の画面で指定した（左側のボックス３００から右側のボックス３０３に抽出した、といってもよい）機能と一致するものが示されている。そして、このプラグインは図示するように、アドレス帳内の全ユーザへのメール送信という必ずしも安全とはいえない処理をおこなうが、それでも使用するかどうかがユーザに問われている。

【００５２】なお、図４のダイアログはプラグインの実行前であればいつ表示してもよいのであるが、現実的には（１）当該プラグインのインストール直前、および／または（２）当該プラグインの起動直前に表示することになる。

【００５３】そして、インストール直前の確認でユーザが「はい」ボタン４００を押下した場合、すなわち警告にもかかわらずユーザが当該プラグインの使用を許可した場合には、実行可否問い合わせ部２０１ｄはさらに図５に示すようなダイアログを表示して、プラグインの起動直前にも再度同様の確認をおこなうかどうかを設定させた後、当該プラグインをインストールする。

【００５４】なお、図４に示すダイアログでユーザが「いいえ」ボタン４０１を押下した場合には、インストールはおこなわずに、「プラグインのインストールを中止しました」などのメッセージを表示する。

【００５５】また、図５に示すダイアログで「はい」ボタン５００が押下された場合、すなわち起動直前にも確認をおこなうよう設定された場合には、この後インストールされたプラグインがそのホストから呼び出される都度、図４と同様のダイアログが表示されるようになる。

【００５６】そして、起動直前に表示された同図のダイアログで「はい」ボタン４００が押下された場合には、図５のダイアログを表示することなく当該プラグインを起動する。また、ここで「いいえ」ボタン４０１が押下されるとプラグインの起動はおこなわず、代わりに「プラグインを起動できませんでした」などのメッセージを表示する。

【００５７】また、図６は同じく実行可否問い合わせ部２０１ｄにより表示される、プラグイン実行中にその実行可否を確認するためのダイアログの一例を示す説明図である。このダイアログはプラグインの実行中、ユーザが図３の画面で指定した機能であって、かつ実行前に提示された機能一覧中にない機能が呼び出されたときに随時表示される。

【００５８】上述した（１）のセキュリティポリシーによる実行前（インストール直前あるいは起動直前）の確認だけでは、プラグインが偽装の機能一覧を提示できるようなウィルスに感染した場合、危険な機能を申告しないことで容易に監視を逃れることができてしまう。そこで上述（２）のセキュリティポリシーにより、実行前に提示されたのと異なる機能が呼び出されていないかどうかを実行中にも常時監視するのである。

【００５９】図６の例では、アドレス帳内の全ユーザへのメール送信は事前には申告されていなかったのであるが、当該プラグインの実行中、上記ダイアログの表示により上記機能の実行は一時保留され、いわば水際で食い止められることになる。

【００６０】なお、図６のダイアログによる警告を受けたユーザは、問題ないと判断すれば「継続」ボタン６００を押下することで、ダイアログで示された処理をそのまま実行させることができる。また、何らかの危険があると判断したときは、「中止」ボタン６０１を押下することでこのプラグインの実行をいったん中断し、プラグインの出所を再確認するなどの対策を取ることができる。

【００６１】もっとも、事前に申告していない機能を呼び出すような怪しいプラグインは一切使用しないという方針であれば、「アンインストール」ボタン６０２を押

下することで、同図のダイアログから直接当該プラグインをアンインストールすることができる。

【００６２】図２に戻り、つぎに２０１ｅはシステム保護部であり、プラグインの実行中その機能呼び出し部２００ｂからいずれかの機能の呼び出しを受け付けると、セキュリティ管理部２０１ａに対して、当該機能がユーザの確認なく実行を許可されるものであるかどうかを問い合わせる。

【００６３】そして上述（２）のセキュリティポリシーのもとで実行が許可される場合、すなわち当該機能が事前に申告されたものである場合には、システム保護部２０１ｅは当該機能をプラグインに提供するいずれかの機能部（後述）に指示して、要求された処理をおこなわせる。

【００６４】また、当該機能の実行が許可されない場合、すなわち当該機能が事前に申告されたものでない場合には、セキュリティ管理部２０１ａからの指示を受けた実行可否問い合わせ部２０１ｄにより、図６に示したようなダイアログが表示される。そして、上述のようにこのダイアログで「継続」ボタン６００が押下されたときに、システム保護部２０１ｅは上記機能をプラグインに提供するいずれかの機能部（後述）に指示して、要求された処理をおこなわせる。

【００６５】図２に戻り、つぎに２０１ｆ～２０１ｉはプラグインに対して各種の機能（サービス）を提供する機能部であり、２０１ｆはファイル読み込みのサービスを提供するファイル読み込み部、２０１ｇはファイル削除のサービスを提供するファイル削除部、２０１ｈはウィンドウ生成のサービスを提供するウィンドウ生成部、２０１ｉはテキスト出力のサービスを提供するテキスト出力部である。なお、提供される機能は上記に掲げたもの以外にも多数存在するが（たとえばレジストリアクセス、メール送信など）、同図では図示を省略している。

【００６６】つぎに、図７～図９は本発明の実施の形態にかかるプログラム実行防止システムにおける、プログラム実行防止処理の手順を示すフローチャートである。図７はプログラム（この場合はプラグイン）のインストールの中止、図８はプログラム（同左）の起動の中止、図９は実行中のプログラム（同左）の中断により、それぞれ結果的に危険なプログラムの実行を阻止するものである。

【００６７】なお、同７～図９のフローチャートによる処理の開始に先立って、セキュリティポリシーＤＢ２０１ｂにはセキュリティポリシー設定部２０１ｃにより、実行前および実行中のセキュリティポリシーがあらかじめ設定されているものとする。

【００６８】まず図７に示す、インストールの中止によるプログラム実行防止の手順について説明する。プラグインの機能一覧提示部２００ａは、当該プラグインのインストールに先立って、そのホストとなるアプリケーションに対して、当該プラグインが呼び出して使用する機能の一覧を提示する（ステップＳ７０１）。

【００６９】ホストとなるアプリケーションは、上記一覧をそのセキュリティ管理部２０１ａで受領するとともに、セキュリティポリシーＤＢ２０１ｂ内のセキュリティポリシーを参照して、このプラグインのインストールにユーザの確認が必要かどうかを判定する（ステップＳ７０２）。具体的には、提示された一覧中にあらかじめ指定された機能が含まれるかどうかをチェックし、含まれていれば確認要、含まれていなければ確認不要とする。

【００７０】そして、ユーザの確認が必要であれば（ステップＳ７０２：Ｙｅｓ）、実行可否問い合わせ部２０１ｄにより図４に示したようなダイアログを表示し（ステップＳ７０３）、同図のダイアログで「はい」ボタン４００が押下されたときは（ステップＳ７０４：Ｙｅｓ）、さらに図５に示したようなダイアログを表示する（ステップＳ７０５）。その後、当該プラグインのインストールを通常通りおこなって（ステップＳ７０６）、本フローチャートによる処理を終了する。

【００７１】また、図４のダイアログで「いいえ」ボタン４０１が押下されたときは（ステップＳ７０４：Ｎｏ）、インストールをおこなう代わりに、インストールを中止した旨のメッセージを表示して（ステップＳ７０７）、本フローチャートによる処理を終了する。

【００７２】つぎに図８に示す、起動の中止によるプログラム実行防止の手順について説明する。プラグインはそのホストとなるアプリケーションから呼び出されると、その機能一覧提示部２００ａにより、使用を予定している機能の一覧を提示する（ステップＳ８０１）。ホストではそのセキュリティ管理部２０１ａにより、このプラグインの起動に先立ってユーザの確認が必要かどうかを判定する（ステップＳ８０２）。

【００７３】具体的には、インストール時の図５のダイアログ（図７のステップＳ７０５）で、起動直前にも再度確認をおこなうように設定されている場合であって、かつ上記で提示された機能一覧中にあらかじめ指定された機能が含まれている場合に、ユーザの確認が必要と判定する（ステップＳ８０２：Ｙｅｓ）。そして実行可否問い合わせ部２０１ｄに指示して、図４に示したようなダイアログを表示させる（ステップＳ８０３）。

【００７４】このダイアログで「はい」ボタン４００が押下されると（ステップＳ８０４：Ｙｅｓ）、プラグインを通常通り起動し（ステップＳ８０５）、「いいえ」ボタン４０１が押下されると（ステップＳ８０４：Ｎｏ）、プラグインの起動を中止した旨のメッセージを表示（ステップＳ８０６）した後、本フローチャートによる処理を終了する。

【００７５】つぎに図９に示す、実行中断によるプログラム実行防止の手順について説明する。プラグインの機

能呼び出し部２００ｂから、そのホストとなるアプリケーションに対して機能の呼び出しがあると（ステップＳ９０１）、システム保護部２０１ｅはセキュリティ管理部２０１ａに指示して、当該機能がユーザの確認なく実行してもよいものであるかどうかを判定させる（ステップＳ９０２）。

【００７６】セキュリティ管理部２０１ａは、当該機能がセキュリティポリシー設定部２０１ｃによりあらかじめ指定された機能であって、かつ実行前（インストール直前および／または起動直前）に提示された機能と異なる場合にユーザの確認が必要と判定し（ステップＳ９０２：Ｙｅｓ）、実行可否問い合わせ部２０１ｄに指示して、図6に示したようなダイアログを表示させる（ステップＳ９０３）。

【００７７】そして、このダイアログで「継続」ボタン６００が押下されると（ステップＳ９０４：Ｙｅｓ）呼び出された処理を実行する、すなわちプラグインの実行をそのまま継続し（ステップＳ９０５）、「中止」ボタン６０１が押下されると（ステップＳ９０４：Ｎｏ、ステップＳ９０６：Ｙｅｓ）、その時点でプラグインの実行を中断するとともにその事実をメッセージにより表示する（ステップＳ９０７）。

【００７８】また、「アンインストール」ボタン６０２が押下されると（ステップＳ９０６：Ｎｏ）、当該プラグインをアンインストール（ステップＳ９０８）した後、本フローチャートによる処理を終了する。

【００７９】なお、上述した実施の形態ではユーザの指示を待ってインストール中止、起動中止あるいは実行中断などをおこなったが、あるいは提示された機能一覧中にあらかじめ指定した機能が含まれていた時点や、あらかじめ提示された機能一覧中にない機能が呼び出された時点で、ユーザの指示を待たず強制的に中止や中断をおこなうようにしてもよい。

【００８０】また、上述した実施の形態ではプログラムが使用する機能単位でユーザに確認するかしないかの設定をおこなったが（図３）、あるいはプログラムごとに確認するかしないかを設定できるようにしてもよい。たとえば一つのＰＣを複数人で使用している場合、他の使用者により危険なプラグイン（出所の定かでないプラグインなど）が安易に導入されることのないように、管理責任者があらかじめプラグインを指定しておき、それ以外のプラグインがインストールされそうになったときに図４のような警告を表示するようにしてもよい。

【００８１】なお、上述の各機能部を実現するプログラムは、ＨＤ１０５のほかＦＤ１０７、ＣＤ－ＲＯＭ１１３あるいはＭＯなどの各種記録媒体に格納することができ、当該記録媒体によって配布することができる。また、ネットワークを介して配布することも可能である。

【００８２】なお、上記説明からも明らかなように、図２に示すセキュリティ管理部２０１ａが請求項にいう「判定手段」「第１の判定手段」および「第２の判定手段」に相当し、そのおこなう処理が請求項にいう「判定工程」「第１の判定工程」および「第２の判定工程」に相当する。

【００８３】また、セキュリティポリシー設定部２０１ｃが請求項にいう「指定手段」に、そのおこなう処理が請求項にいう「指定工程」に相当する。さらに、実行可否問い合わせ部2.０１ｄが請求項にいう「問い合わせ手段」に、そのおこなう処理が請求項にいう「問い合わせ工程」に相当する。

【００８４】以上説明したように本発明の実施の形態によれば、ユーザやシステムにダメージを与えるおそれのある機能がプラグイン中に含まれる場合に、ユーザの判断にしたがって当該プラグインのインストールや起動が拒否されるので、当該プラグインが実行された結果生ずるかもしれない損害を未然に回避することができる。

【００８５】また、実行前に提示された機能一覧を安易に信用することなく、実行中にもその信憑性を常時監視しているため、事前に申告していない危険な機能を実行中にひそかに呼び出そうとするようなプラグインを、当該機能が呼び出される直前に停止させることができる。これによりもたらされる効果は上記と同様である。

【００８６】そして、本発明はその原理上、ウィルスに感染したプログラムであるか何らかの悪意をもって作成されたプログラムであるかを問わず、ユーザやシステムにとって危険な動作をするものであればその実行を阻止することができるので、従来技術で指摘困難だった、通常のプログラムと区別のつかない悪意のあるプログラムも容易に検出することができる。

【００８７】また、近年増加している多形態型のウィルスであっても、その目的とする処理が同一である限り、表面的なコードの差異にかかわらず検出できるという特長を持っている。しかもその検出のために、すべてのウィルスのコード群を網羅したウィルス定義ファイル（パターンファイル、ＤＡＴファイルなどともいう）を用意する必要はなく、また当該ファイルを頻繁に更新する作業も不要である。

【００８８】また、本発明は上述のように、呼び出し予定の機能の中に危険なものが含まれるか、実際に呼び出された機能が事前に申告されていたかといった、ごく単純な判定によりプログラムの実行を阻止するので、従来のウィルススキャンのように長時間を要することなく、日々無理なく励行され実効性がはかれるという現実的なメリットもある。

【００８９】また、従来技術のＪａｖａのように使用できる機能を一律に制限するものではないので、プログラムの自由度が増し、安全性と利便性の両立をはかることが可能である。

【００９０】なお、上述した実施の形態ではプログラムの中でも特にプラグインについて、そのホストとなるア

プリケーションにおいて実行可否を判定するようにしたが、たとえばマクロと当該マクロの動作するアプリケーションとの関係に本発明を応用することも可能である。

【００９１】また、一般のアプリケーションとＯＳとの間に本発明を適用する、すなわちＯＳそのものにプログラムのインストールの中止や起動の中止、あるいは実行中のプログラムの中断の機能を持たせることもできる。これにより、別途アンチウィルスソフトなどを導入するのと同等の、あるいはそれ以上の危険防止効果が得られることになる。

【００９２】図１０は、本発明によるプログラム実行防止機能をＯＳに具備させた場合に、アプリケーションの実行がどのように阻止されるかを模式的に示す説明図である。同図は偽装の機能一覧の提示により、いったんインストールおよび起動を許可されたアプリケーションが、実行中に上記一覧中にない、ファイル削除機能を呼び出した時点で中断される例を示している。

【００９３】

【発明の効果】以上説明したように請求項１に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ手段と、を備えたので、あらかじめ指定された処理をおこなうプログラムについては、インストールに先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該インストールが中止され、これによって、ユーザやシステムにとって危険なプログラムの実行を未然に防止することが可能なプログラム実行防止装置が得られるという効果を奏する。

【００９４】また、請求項２に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから提示された機能一覧中に前記指定手段により指定された機能が含まれるか否かを判定する判定手段と、前記判定手段により前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ手段と、を備えたので、あらかじめ指定された処理をおこなうプログラムについては、起動に先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該起動が中止され、これによって、ユーザやシステムにとって危険なプログラムの実行を未然に防止することが可能なプログラム実行防止装置が得られるという効果を奏する。

【００９５】また、請求項３に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定手段と、プログラムから呼び出された機能が前記指定手段により指定された機能であるか否かを判定する第１の判定手段と、前記第１の判定手段により前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていたか否かを判定する第２の判定手段と、前記第２の判定手段により前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ手段と、を備えたので、プログラムの実行中あらかじめ提示されたのとは異なる機能が呼び出されたときは、ユーザにその事実が警告されるとともに、ユーザが指示した場合には当該プログラムの実行が中断され、これによって、ユーザやシステムにとって危険なプログラムの問題部分の実行を未然に防止することが可能なプログラム実行防止装置が得られるという効果を奏する。

【００９６】また、請求項４に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムをインストールするか否かをユーザに問い合わせる問い合わせ工程と、を含んだので、あらかじめ指定された処理をおこなうプログラムについては、インストールに先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該インストールが中止され、これによって、ユーザやシステムにとって危険なプログラムの実行を未然に防止することが可能なプログラム実行防止方法が得られるという効果を奏する。

【００９７】また、請求項５に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから提示された機能一覧中に前記指定工程で指定された機能が含まれるか否かを判定する判定工程と、前記判定工程で前記機能一覧中に前記指定された機能が含まれると判定された場合に、前記プログラムを起動するか否かをユーザに問い合わせる問い合わせ工程と、を含んだので、あらかじめ指定された処理をおこなうプログラムについては、起動に先立ってユーザにその事実が警告されるとともに、ユーザが指示した場合には当該起動が中止され、これによって、ユーザやシステムにとって危険なプログラムの実行を未然に防止することが可能なプログラム実行防止方法が得られるという効果を奏する。

【００９８】また、請求項６に記載の発明は、その実行にユーザの許可が必要な機能を指定する指定工程と、プログラムから呼び出された機能が前記指定工程で指定された機能であるか否かを判定する第１の判定工程と、前記第１の判定工程で前記呼び出された機能が前記指定された機能であると判定された場合に、前記呼び出された機能が前記プログラムから提示された機能一覧中に含ま

れていたか否かを判定する第２の判定工程と、前記第２の判定工程で前記呼び出された機能が前記プログラムから提示された機能一覧中に含まれていなかったと判定された場合に、前記プログラムの実行を継続するか否かをユーザに問い合わせる問い合わせ工程と、を含んだので、プログラムの実行中あらかじめ提示されたのとは異なる機能が呼び出されたときは、ユーザにその事実が警告されるとともに、ユーザが指示した場合には当該プログラムの実行が中断され、これによって、ユーザやシステムにとって危険なプログラムの問題部分の実行を未然に防止することが可能なプログラム実行防止方法が得られるという効果を奏する。

【００９９】また、請求項７に記載の発明は、前記請求項４～請求項６のいずれか一つに記載の方法をコンピュータに実行させるので、前記請求項４～請求項６のいずれか一つに記載の方法がコンピュータにより読み取られて実行され、これによって、ユーザやシステムにとって危険なプログラム、あるいは少なくともその問題部分の実行を未然に防止することが可能なプログラムが得られるという効果を奏する。

【０１００】また、請求項８に記載の発明は、前記請求項７に記載のプログラムを記録したので、前記請求項７に記載のプログラムがコンピュータにより読み取られて実行され、これによって、ユーザやシステムにとって危険なプログラム、あるいは少なくともその問題部分の実行を未然に防止することが可能な記録媒体が得られるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の実施の形態にかかるプログラム実行防止装置のハードウェア構成を示す説明図である。

【図２】本発明の実施の形態にかかるプログラム実行防止装置の構成を機能的に示す説明図である。

【図３】セキュリティポリシー設定部２０１ｃにより表示される、セキュリティポリシーの詳細を設定するための画面の一例を示す説明図である。

【図４】実行可否問い合わせ部２０１ｄにより表示される、プラグイン実行前にその実行可否を確認するためのダイアログの一例を示す説明図である。

【図５】実行可否問い合わせ部２０１ｄにより表示される、プラグインの起動直前にも実行可否を確認するかどうかを設定するためのダイアログの一例を示す説明図である。

【図６】実行可否問い合わせ部２０１ｄにより表示される、プラグイン実行中にその実行可否を確認するためのダイアログの一例を示す説明図である。

【図７】本発明の実施の形態にかかるプログラム実行防止システムにおける、インストールの中止によるプログラム実行防止処理の手順を示すフローチャートである。

【図８】本発明の実施の形態にかかるプログラム実行防止システムにおける、起動中止によるプログラム実行防止処理の手順を示すフローチャートである。

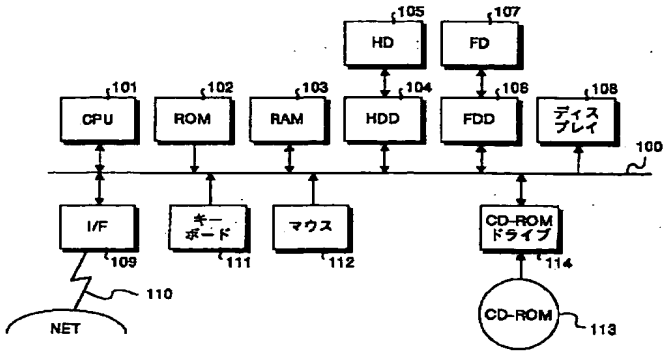
【図９】本発明の実施の形態にかかるプログラム実行防止システムにおける、実行中断によるプログラム実行防止処理の手順を示すフローチャートである。

【図１０】本発明をＯＳに応用した場合にアプリケーションの実行がどのように阻止されるかを模式的に示す説明図である。

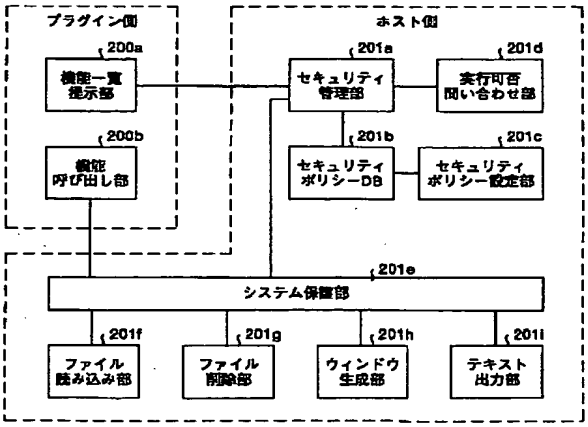
【符号の説明】

１００　バスまたはケーブル
１０１　ＣＰＵ
１０２　ＲＯＭ
１０３　ＲＡＭ
１０４　ＨＤＤ
１０５　ＨＤ
１０６　ＦＤＤ
１０７　ＦＤ
１０８　ディスプレイ
１０９　ネットワークＩ／Ｆ
１１０　通信ケーブル
１１１　キーボード
１１２　マウス
１１３　ＣＤ－ＲＯＭ
１１４　ＣＤ－ＲＯＭドライブ
２００ａ　機能一覧提示部
２００ｂ　機能呼び出し部
２０１ａ　セキュリティ管理部
２０１ｂ　セキュリティポリシーＤＢ
２０１ｃ　セキュリティポリシー設定部
２０１ｄ　実行可否問い合わせ部
２０１ｅ　システム保護部
２０１ｆ　ファイル読み込み部
２０１ｇ　ファイル削除部
２０１ｈ　ウィンドウ生成部
２０１ｉ　テキスト出力部

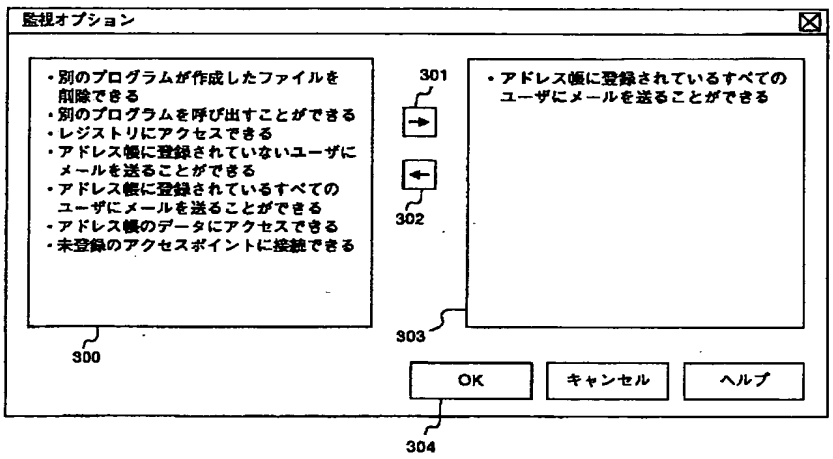
【図１】


HD
FD
CPU
ROM
RAM
HDD
FDD
ディスプレイ
100
I/F
キーボード
マウス
CD-ROMドライブ
109
111
112
114
110
NET
CD-ROM
113

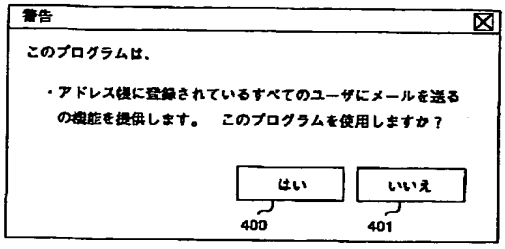
【図２】


プラグイン側
ホスト側
機能一覧提示部
機能呼び出し部
セキュリティ管理部
実行可否問い合わせ部
セキュリティポリシーDB
セキュリティポリシー設定部
システム保管部
ファイル読み込み部
ファイル削除部
ウィンドウ生成部
テキスト出力部

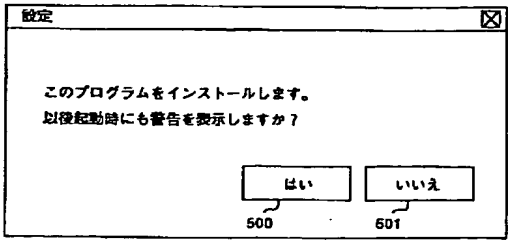
【図３】


監視オプション
・別のプログラムが作成したファイルを削除できる
・別のプログラムを呼び出すことができる
・レジストリにアクセスできる
・アドレス帳に登録されていないユーザにメールを送ることができる
・アドレス帳に登録されているすべてのユーザにメールを送ることができる
・アドレス帳のデータにアクセスできる
・未登録のアクセスポイントに接続できる
・アドレス帳に登録されているすべてのユーザにメールを送ることができる
OK
キャンセル
ヘルプ

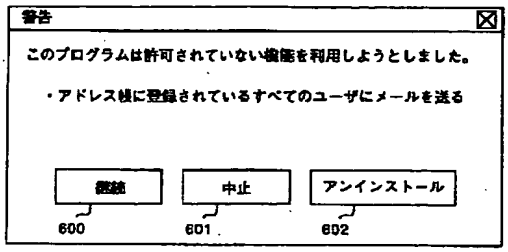
【図４】


警告
このプログラムは、
・アドレス帳に登録されているすべてのユーザにメールを送るの機能を提供します。 このプログラムを使用しますか？
はい
いいえ

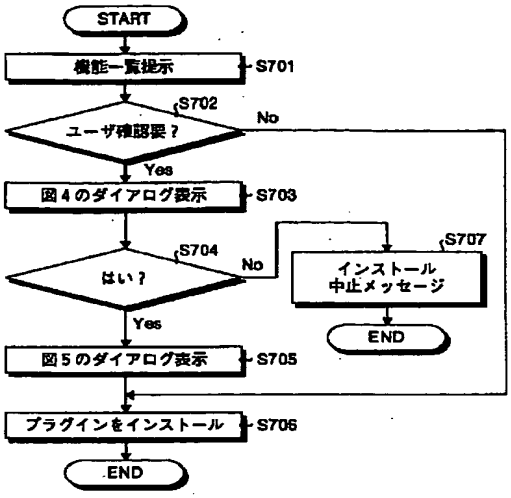
【図５】


設定
このプログラムをインストールします。
以後起動時にも警告を表示しますか？
はい
いいえ

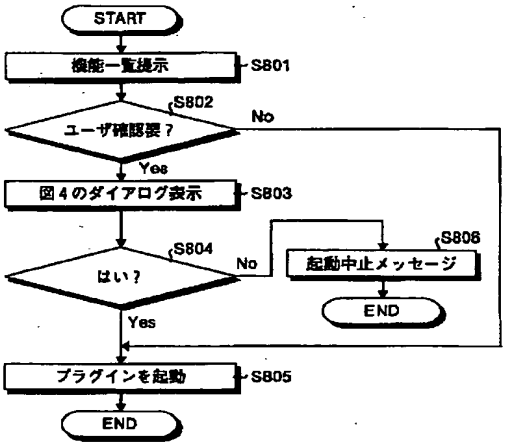
【図６】


警告
このプログラムは許可されていない機能を利用しようとしました。
・アドレス帳に登録されているすべてのユーザにメールを送る
継続
中止
アンインストール
600
601
602

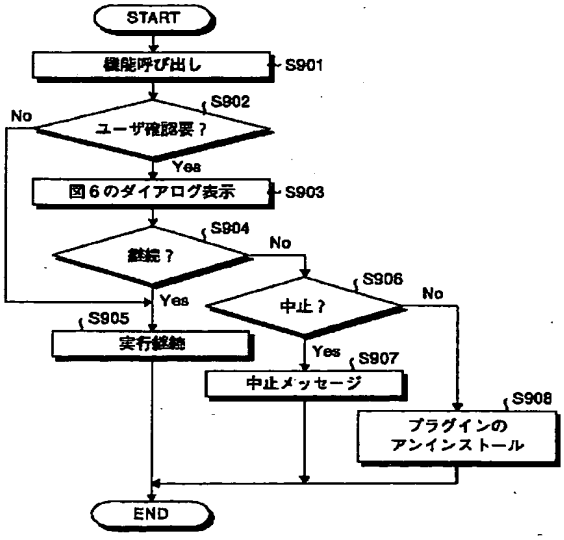
【図７】


START
機能一覧提示
S701
S702
ユーザ確認要？
No
Yes
図４のダイアログ表示
S703
S704
はい？
No
S707
インストール
中止メッセージ
END
Yes
図５のダイアログ表示
S705
プラグインをインストール
S706
END

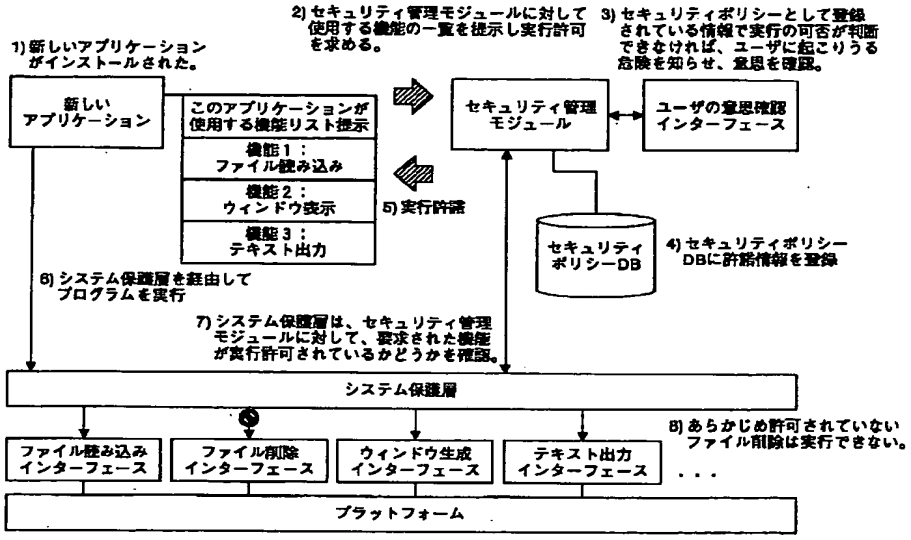
【図８】


START
機能一覧提示
S801
S802
ユーザ確認要？
No
Yes
図４のダイアログ表示
S803
S804
はい？
No
S806
起動中止メッセージ
END
Yes
プラグインを起動
S805
END

【図９】


START
機能呼び出し
S901
S902
No
ユーザ確認要？
Yes
図６のダイアログ表示
S903
S904
継続？
No
S906
No
Yes
中止？
S905
実行継続
Yes
S907
中止メッセージ
S908
プラグインの
アンインストール
END

【図１０】


1) 新しいアプリケーションがインストールされた。
2) セキュリティ管理モジュールに対して使用する機能の一覧を提示し実行許可を求める。
3) セキュリティポリシーとして登録されている情報で実行の可否が判断できなければ、ユーザに起こりうる危険を知らせ、意思を確認。
新しいアプリケーション
このアプリケーションが使用する機能リスト提示
機能１：ファイル読み込み
機能２：ウィンドウ表示
機能３：テキスト出力
セキュリティ管理モジュール
ユーザの意思確認インターフェース
5) 実行許諾
セキュリティポリシーDB
4) セキュリティポリシーDBに許諾情報を登録
6) システム保護層を経由してプログラムを実行
7) システム保護層は、セキュリティ管理モジュールに対して、要求された機能が実行許可されているかどうかを確認。
システム保護層
8) あらかじめ許可されていないファイル削除は実行できない。
ファイル読み込みインターフェース
ファイル削除インターフェース
ウィンドウ生成インターフェース
テキスト出力インターフェース
・・・
プラットフォーム